BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Dinas Komunikasi dan Informatika Kota Tasikmalaya

Dinas Komunikasi dan Informatika mempunyai tugas pokok membantu Walikota melaksanakan urusan pemerintahan daerah dan tugas pembantuan di bidang komunikasi dan informatika, statistik serta persandian.

Gambar 2.1 Logo Dinas Komunikasi dan Informatika (Diskominfo, 2024)

Fungsi Dinas Komunikasi dan Informatika dalam melaksanakan tugas pokok sebagaimana dimaksud dalam Pasal 78, menyelenggarakan fungsi:

1. Perumusan kebijakan dalam penyelenggaraan urusan komunikasi dan informatika, statistik serta persandian.
2. Pelaksanaan kebijakan penyelenggaraan urusan komunikasi dan informatika, statistik serta persandian.
3. Pelaksanaan evaluasi dan pelaporan sesuai dengan lingkup tugasnya.

4. Pelaksanaan pengelolaan administrasi dinas.

5. Pelaksanaan fungsi lain yang diberikan oleh Walikota sesuai tugas dan fungsinya.

2.1.2 Keamanan Informasi

Informasi menjadi aset berharga bagi suatu organisasi karena berfungsi sebagai salah satu sumber daya strategis untuk meningkatkan nilai usaha. Oleh karena itu, perlindungan informasi, yang mencakup kebijakan, prosedur, proses, dan aktivitas, menjadi hal yang sangat penting untuk diperhatikan secara serius oleh seluruh pemilik, manajemen, dan karyawan organisasi terkait. Keamanan informasi ini merujuk pada upaya melindungi informasi dari berbagai ancaman potensial yang dapat menimbulkan kerugian bagi kelangsungan hidup organisasi(Novianto, 2020). Menurut (Basatha et al., 2023) Prinsip keamanan adalah sebagai berikut:

1. *Confidentiality:* merupakan faktor terkait jaminan terhadap kerahasiaan suatu data atau informasi, secara aktivitas keamanan terhadap data dan informasi dapat dengan cara memberi kepastian bahwa akses informasi hanya dapat dilakukan oleh orang yang ditunjuk atau yang memiliki wewenang serta menjamin kerahasiaan terhadap proses pengiriman data, proses penerimaan data dan proses penyimpanan data.

2. *Integrity:* adalah aspek yang memastikandata harus terjaga keakuratan dan keutuhan informasinya serta tidak dapat dirubah tanpa ada ijin atau otoritas dari pihak yang berwenang

3. *Availability:* aspek yang memberikan kepastian bahwa seorang penggunaberhak dalam menggunakan informasi dan perangkat apabila diperlukan dan memastikan pula bahwa data tersedia dan siap digunakan saat dibutuhkan

2.1.3 Sistem Pemerintahan Berbasis Elektronik (SPBE)

Pengertian SPBE menurut Pasal 1 ayat 1 Perpres No 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik adalah penyelenggaraan pemerintah yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE. Ruang lingkup pedoman evaluasi SPBE meliputi penilaian tingkat organisasi mencakup Instansi Pusat (Kementerian dan Lembaga) dan Pemerintah Daerah (pemerintah provinsi dan pemerintah kabupaten/kota). Pada umumnya, pelayanan Sistem Pemerintahan Berbasis Elektronik (SPBE) ditujukan untuk melayani kebutuhan publik dan administrasi pemerintahan. Pengguna layanan SPBE ini mencakup berbagai pihak, seperti instansi pemerintah, aparatur sipil negara, pelaku bisnis, masyarakat, dan entitas lainnya. Untuk memastikan kelancaran operasional sistem pemerintahan berbasis elektronik, diperlukan tata kelola, infrastruktur, dan sumber daya manusia yang handal.

2.1.4 STANDAR SNI ISO/IEC 27001

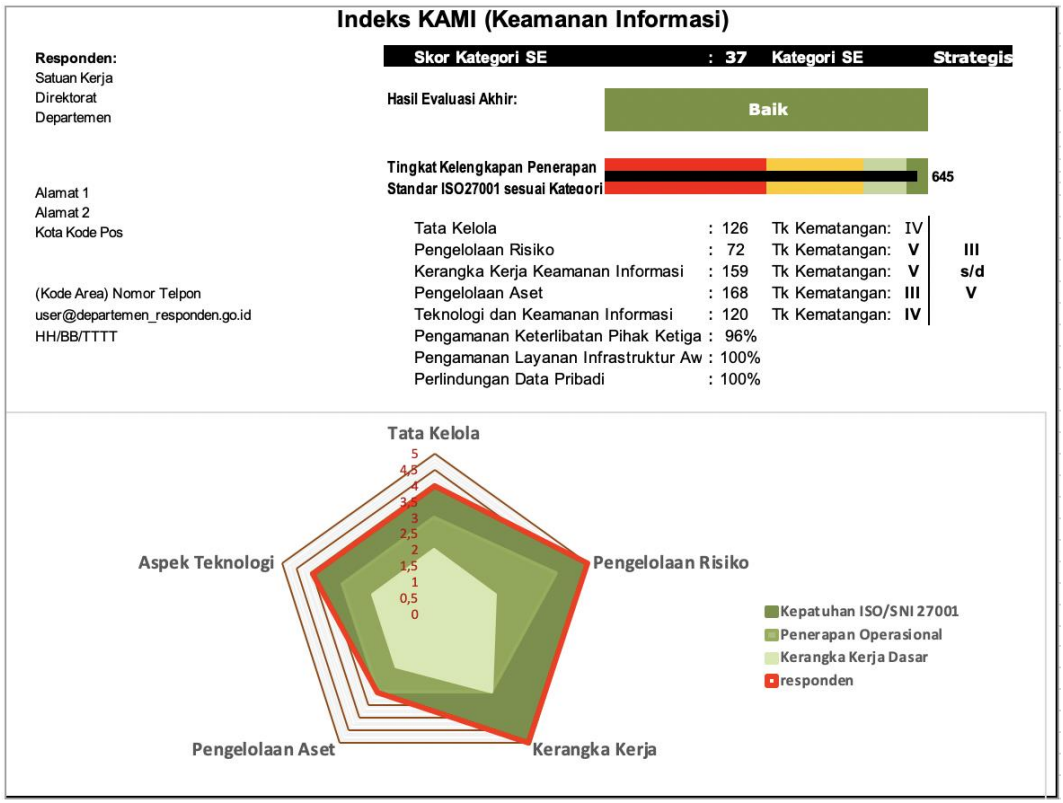
ISO/IEC 27001 adalah sebuah standar keamanan informasi yang mencakup prinsip-prinsip dasar Sistem Manajemen Keamanan Informasi (SMKI). Standar ini mengadopsi pendekatan manajemen berdasarkan kontrol yang didasarkan pada analisis risiko. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality*, *integrity* dan *availability*. ISO/EIC 27001:2022 merupakan versi terbaru dari standar internasional yang mengatur

penerapan Sistem Manajemen Keamanan Informasi (ISMS). Standar ini memberikan kerangka kerja menyeluruh bagi organisasi dalam mengenali, mengendalikan, dan meminimalkan risiko yang berkaitan dengan keamanan informasi(Sinaga & Taan, 2024). *Framework* tersebut menerapkan prinsip-prinsip dasar *Information Security Management Systems PDCA(Plan-Do-Check-Act)* dan ISO 27001 merupakan salah satu standar *framework* yang paling terkenal karena tidak hanya diterapkan di organisasi Amerika Serikat, tetapi di seluruh dunia(Paradise et al., 2018). Model ini adalah model yang digunakan dalam pelaksanaan sistem manajemen keamanan informasi atau sering disebut sebagai siklus SMKI. Model PDCA diciptakan untuk mendorong perbaikan yang berkelanjutan. Dengan menerapkan SMKI sesuai dengan yang dijelaskan dalam standar ISO/IEC 27001:2022, sebuah organisasi dapat menggunakan model PDCA(Haqqi et al., 2022).

2.1.5 Indeks Keamanan Informasi (Indeks KAMI)

Alat evaluasi yang disebut sebagai Indeks Keamanan Informasi (KAMI) telah dibuat dengan tujuan untuk mengevaluasi kesiapan instansi pemerintah terhadap keamanan informasi. Meskipun tidak dimaksudkan untuk menilai apakah bentuk keamanan yang sudah ada layak atau efektif, alat ini berfungsi sebagai instrumen yang memberikan gambaran umum tentang kesiapan (tingkat kematangan dan kelengkapan) struktur keamanan informasi kepada pemimpin organisasi (Rahayu et al., 2021). Disarankan agar evaluasi menggunakan Indeks KAMI dilakukan oleh pejabat yang memiliki tanggung jawab langsung dan kewenangan dalam mengelola

keamanan informasi di seluruh lingkup instansi tersebut(Dwi Prasetyowati et al., 2019).



Gambar 2. 2 Diagram Indeks KAMI (BSSN, 2024)

Proses evaluasi Indeks KAMI versi 5.0 melibatkan sejumlah pertanyaan yang mencakup beberapa area berikut yaitu kategori sistem elektronik yang digunakan, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, perlindungan data pribadi, serta suplemen (pengukuran tambahan untuk aspek pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan (*cloud service*), dan perlindungan data pribadi).

Tingkat kematangan ini akan berfungsi sebagai instrumen untuk melaporkan pemetaan dan peringkat kesiapan keamanan informasi di Kementerian/Lembaga. Dalam konteks Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai berikut:

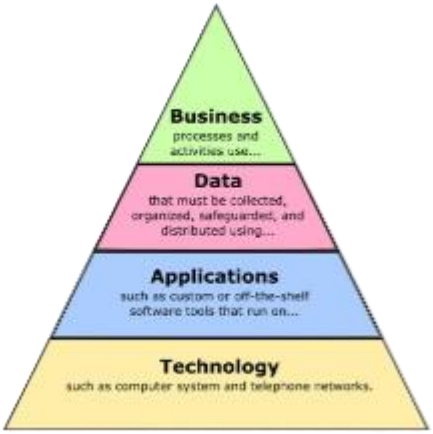
1. Tingkat I – Kondisi Awal
2. Tingkat II – Penerapan Kerangka Kerja Dasar
3. Tingkat III – Terdefinisi dan Konsisten
4. Tingkat IV – Terkelola dan Terukur
5. Tingkat V – Optimal

Demi memberikan penjelasan yang lebih rinci, tingkatan tersebut diperluas dengan penambahan tingkat antara, yaitu I+, II+, III+, dan IV+, sehingga secara total terdapat 9 tingkatan kematangan. Pada tahap awal, semua responden akan dikategorikan dalam tingkatan kematangan Tingkat I. Sejalan dengan standar ISO/IEC 27001, tingkatan kematangan yang diinginkan untuk mencapai ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

2.1.6 *Enterprise Architecture* (EA)

"Enterprise" merujuk pada sekelompok organisasi atau pemerintah yang memiliki tujuan bersama. *"Architecture"* dalam konteks ini mengacu pada deskripsi dari segi perusahaan atau organisasi, mencakup gambaran bangunan dan struktur, gaya desain, serta metode konstruksi fisik dan elemen-elemen lainnya. *Enterprise Architecture* adalah suatu kerangka kerja yang terdiri dari metode, prinsip, dan model yang membantu dalam merancang serta mewujudkan struktur organisasi, proses bisnis, sistem informasi, dan infrastruktur di suatu perusahaan. Tujuan

utamanya adalah mencapai keselarasan antara bisnis dan teknologi informasi. *Enterprise Architecture* menghasilkan gambaran rinci atau *blue print* untuk mengatur semua proses bisnis di perusahaan, teknologi pendukung, dan informasi yang diperlukan(Fikri et al., 2023).



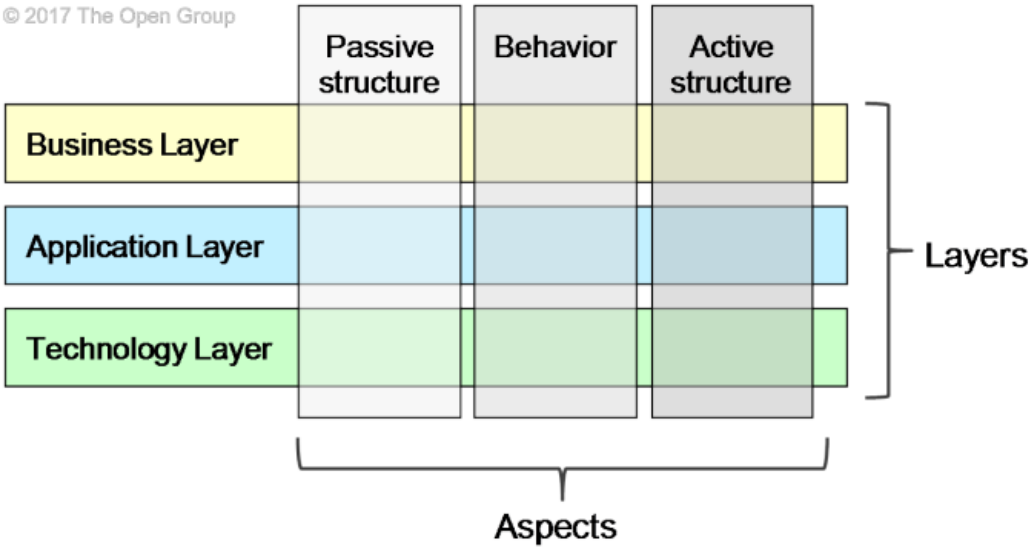
Gambar 2. 3 Lapisan *Enterprise Architecture*

Pemahaman lain dari *Enterprise Architecture* adalah sebagai suatu proses analisis dan penyusunan dokumen mengenai organisasi, baik pada keadaan saat ini maupun keadaan di masa depan, yang dilihat dari perspektif strategi, bisnis, dan teknologi yang terintegrasi. *Enterprise Architecture* merupakan praktik manajemen dan teknologi yang bertujuan untuk meningkatkan kinerja organisasi dengan mengevaluasi situasi organisasi secara komprehensif dan terpadu, mencakup aspek strategis, praktik bisnis, aliran informasi, dan sumber daya teknologi (Yulianti et al., 2020).

2.1.7 *ArchiMate*

Tim proyek Telematica Institut pertama kali mengusulkan *ArchiMate* pada tahun 2002, dan kemudian alat pemodelan tersebut diakuisisi oleh The Open Group

(TOG). TOG kemudian merilis kembali alat pemodelan tersebut sebagai *ArchiMate* 1.0 pada tahun 2009. *ArchiMate* adalah bahasa pemodelan untuk *Enterprise Architecture* yang menyediakan sebuah instrumen untuk mendeskripsikan dan memvisualisasikan hubungan antar domain dengan cara yang jelas.



Gambar 2. 4 *ArchiMate* Core Framework

ArchiMate dapat dijelaskan dalam dua tingkat kompleksitas. Pertama, kerangka inti *ArchiMate* yang mendefinisikan konsep dan hubungan yang diperlukan untuk memodelkan EA. kerangka kerja terdiri dari tiga lapisan – *Business Layer, Application Layer*, dan *Technology Layer* dan tiga elemen lintas sektor – *Passive Structrure, Behavior,* dan *Active structure* (Nurul Mutiah, Indah Zulfah Alqadrie, 2020)

2.2 State of the Art

No	Penelitian Terdahulu (Penulis, Tahun)	Fokus/Metode	Kelemahan/GAP	Keterebaruan Penelitian
1	(Dewantara & Sugiantoro, 2021)	Evaluasi keamanan informasi UIN menggunakan Indeks KAMI dan OSSIM	Tidak menyajikan hasil dalam bentuk pemodelan EA atau *ArchiMate*	Evaluasi disajikan menggunakan *ArchiMate*
2	(Wijaya, 2021)	Evaluasi sistem Pasdeal dengan Indeks KAMI & ISO 27001:2013	Hanya fokus pada penerapan ISO dan nilai evaluasi, tanpa visualisasi arsitektur	Menyediakan pemodelan arsitektur menggunakan *ArchiMate*
3	(Prince Sales et al., 2018)	Analisis ontologi risiko pada *ArchiMate*	Fokus hanya pada aspek risiko, tidak membahas evaluasi menyeluruh keamanan informasi	Menggabungkan hasil evaluasi lengkap dengan visualisasi *ArchiMate*
4	(Zhi & Zhou, 2022)	Pemodelan empiris EA dengan *ArchiMate*	Tidak membahas evaluasi keamanan informasi; hanya aspek pemodelan umum	Menggunakan *ArchiMate* untuk visualisasi hasil evaluasi keamanan SPBE

5	(Haikal et al., 2019)	Perancangan tata kelola SPBE dengan ISO 27001:2013	Tidak menggunakan Indeks KAMI; tidak memodelkan secara visual	Menggunakan Indeks KAMI versi terbaru & pemodelan *ArchiMate*
6	(Saputro et al., 2023)	Analisis dan desain arsitektur EA SPBE di BPKD	Fokus pada domain aplikasi; tidak menggunakan Indeks KAMI	Fokus evaluasi keamanan + pemodelan EA dalam satu pendekatan
7	(Saputra et al., 2023)	Evaluasi keamanan informasi Kominfo XYZ dengan Indeks KAMI 4.2	Menggunakan versi lama Indeks KAMI; tidak menyajikan visualisasi	Menggunakan Indeks KAMI 5.0 & visualisasi dengan *ArchiMate*
8	(A. Ellerm & Morales-Trujillo, 2020)	Studi sistematis pemodelan aspek keamanan dengan *ArchiMate*	Masih dalam tahap sistematik dan eksploratif; belum diimplementasikan	Implementasi nyata pemodelan keamanan SPBE
9	(A. W. Ellerm & Morales-Trujillo, 2021)	Penggunaan *ArchiMate* untuk mikromobilitas	Fokus sektor privat dan mikromobilitas; bukan pada sistem pemerintahan	Diterapkan pada instansi pemerintahan daerah (Diskominfo)
10	(Korman et al., 2014)	Evaluasi kebutuhan informasi dalam penilaian risiko	Tidak menyajikan evaluasi komprehensif sistem informasi SPBE	Evaluasi keamanan sistem SPBE secara menyeluruh dan visual

2.3 Keterbaruan Penelitian

Keterbaruan dari penelitian yang dilakukan yaitu evaluasi keamanan SPBE pada Dinas Komunikasi dan Informatika Kota Tasikmalaya menggunakan Indeks KAMI dan menyajikan hasil evaluasi menggunakan pemodelan *ArchiMate Enterprise Architecture*.

Tabel 2.1 Matriks Penelitain

Penelitian	**Ruang Lingkup**				
	SPBE	***Indeks KAMI***	***Standar ISO IEC 27001***	***ArchiMate***	***Enterprise Architecture***
Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Jaringan (Studi Kasus : UIN Sunan Kalijaga Yogyakarta) (Dewantara & Sugiantoro, 2021)		✓	✓		
Evaluasi Keamanan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013 (Wijaya, 2021)		✓	✓		
Ontological Analysis And Redesign Of Risk Modeling In ArchiMate (Prince Sales et al., 2018)				✓	✓
Empirically Modeling Enterprise Architecture Using ArchiMate (Zhi & Zhou, 2022)				✓	✓
Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2013 (STUDI KASUS: DISKOMINFOTIK KABUPATEN BANDUNG BARAT) (Haikal et al., 2019)	✓		✓		

Penelitian	Ruang Lingkup				
	SPBE	***Indeks KAMI***	***Standar ISO IEC 27001***	***ArchiMate***	***Enterprise Architecture***
Analisis dan Perancangan Arsitektur Enterprise Sistem Pemerintahan Berbasis Elektronik (SPBE) Pada Domain Aplikasi di Lingkungan Badan Pengelolaan Keuangan Daerah (BPKD) (Saputro et al., 2023)	✓				
Penilaian Tingkat Kesiapan Keamanan Informasi Pada Dinas Kominfo Kabupaten XYZ Dengan Indeks Kami Versi 4.2 (Saputra et al., 2023)		✓	✓		
Modelling Security Aspects with ArchiMate: A Systematic Mapping Study (A. Ellerm & Morales-Trujillo, 2020)				✓	✓
Utilising The ArchiMate Framework To Model Secure Micromobility Services (A. W. Ellerm & Morales-Trujillo, 2021)				✓	✓
Overview of Enterprise Information Needs in Information Security Risk Assessment (Korman et al., 2014)				✓	✓
Evaluasi Keamanan Sistem Pemerintahan Berbasis Elektronik Menggunakan Indeks Kami Dan Pemodelan *ArchiMate Enterprise Architecture*	✓	✓	✓	✓	✓

Berdasarkan penelitian terkait, hasil dari evaluasi keamanan terdapat keterbatasan indeks KAMI yang hanya menampilkan aspek penilaian nya saja dan tidak ada ketentuan dalam penyusunan rekomendasi perbaikan. Sehingga peneliti

mengusulkan akan melakukan evaluasi keamanan SPBE menggunakan indeks KAMI dan menyajikan hasil dengan pemodelan *ArchiMate*.